



IDÉE 2

L'IA POURRAIT RENFORCER LES ACTEURS NON ÉTATIQUES ET SUBMERGER LES ORGANISATIONS DE SÉCURITÉ

À l'avenir, l'IA plus accessible et plus polyvalente aura des répercussions sur la sécurité. Les acteurs non étatiques, bons ou mauvais, auront accès à des capacités traditionnellement détenues uniquement par les États. Ils pourraient être en mesure de les déployer plus rapidement que les États, ce qui maintiendrait les organisations de sécurité dans une course constante pour les rattraper.

AUJOURD'HUI

L'IA abaisse les barrières à l'accès et réduit le coût des attaques¹. Par exemple, l'IA peut aider une personne ayant des compétences limitées en programmation à concevoir des logiciels malveillants². Les principaux modèles d'IA à code source ouvert ont des capacités légèrement inférieures à celles de l'IA polyvalente la plus puissante, GTP-4 Turbo³. Leur caractère polyvalent les rend également utiles pour tous les types de problèmes, y compris les activités nuisibles. On ne sait pas qui utilisera l'IA le plus efficacement et le plus rapidement : les organes gouvernementaux des nations rivales ou les acteurs non étatiques⁴. Toutefois, l'IA pourrait habiliter des acteurs non étatiques, des entreprises ou des nations qui ne sont pas soumis à des contraintes juridiques ou éthiques et qui sont prêts à appliquer la technologie d'une manière que d'autres États ne peuvent pas adopter.





AVENIRS

De nombreux nouveaux acteurs pourraient avoir accès à la surveillance à grande échelle à l'avenir. La capacité de l'IA à analyser de grandes quantités de données de sources ouvertes pourrait permettre à de nouveaux acteurs de suivre et de prévoir les mouvements des forces policières et militaires⁵. Les outils d'IA peuvent aider à écrire des codes informatiques malveillants, ce qui rend la cyberdéfense plus difficile. De même, ChatGPT a été utilisé pour créer des logiciels malveillants évolutifs, c'est-à-dire des logiciels malveillants capables de modifier leur code d'origine pour échapper aux cyberdéfenses⁶.

L'IA peut également être utilisée dans le cadre d'attaques non conventionnelles, afin de réduire le coût des dommages physiques ou des attaques contre les infrastructures. Par exemple, l'IA peut faciliter le processus d'impression 3D de pièces dangereuses, comme celles nécessaires à la fabrication d'armes nucléaires⁷. L'IA pourrait également être utilisée pour automatiser des essaims de drones bon marché afin d'écraser les défenses aériennes⁸, ce qui donnerait un avantage aux acteurs plus petits qui souhaitent cibler les zones urbaines ou affronter les armées modernes. Si l'IA augmente considérablement l'accès et automatise les dommages, cela pourrait accroître la pression sur le secteur de la sécurité et modifier la manière dont il assure la sécurité des citoyens.



IMPLICATIONS

- L'IA à code source ouvert pourrait donner aux acteurs non étatiques de nouveaux outils et **éroder les avantages traditionnellement détenus par les États**, tels que la surveillance et le contrôle⁹
- **La capacité des organismes d'application de la loi à recueillir des renseignements pourrait être limitée** par rapport à celle des acteurs non étatiques
- Davantage de communautés pourraient contester l'utilisation de l'IA par les organismes d'application de la loi
- L'utilisation innovante de l'IA pourrait **dépasser la capacité d'adaptation des organisations de défense et de sécurité**. Les échecs en matière de sécurité publique pourraient affaiblir la confiance des institutions ou modifier l'attitude du public quant à l'utilisation appropriée de l'IA par les pouvoirs publics¹⁰
- Les entreprises privées spécialisées dans l'IA pourraient devenir les principaux acteurs des secteurs de la cybersécurité et du renseignement, y compris dans des espaces traditionnellement considérés comme relevant du domaine public

Notes de fin de texte

- 1 Kreps, Sarah et Li, Richard. « [Cascading Chaos: Nonstate Actors and AI on the Battlefield](#) ». Brookings, 1^{er} février 2022.
- 2 Scroxton, Alex. « [Research Team Tricks AI Chatbots into Writing Usable Malicious Code](#) ». Computer Weekly, 24 octobre 2023.
- 3 Huggingface. « [LMSys Chatbot Arena Leaderboard - a Hugging Face Space by Lmsys](#) ». Consulté le 19 février 2024.
- 4 Hirsh, Michael. « [How AI Will Revolutionize Warfare](#) ». Foreign Policy (blogue), 11 avril 2023.
- 5 Homeland Security. « [Addressing Risks From Non-State Actors' Use of Commercially Available Technologies](#) », 2022.
- 6 Mascellino, Alessandro. « [ChatGPT Creates Polymorphic Malware](#) ». Infosecurity Magazine, 18 janvier 2023.
- 7 Volpe, Tristan. « [Dual-Use Distinguishability: How 3D-Printing Shapes the Security Dilemma for Nuclear Programs](#) ». Fondation Carnegie pour la paix internationale. Consulté le 19 février 2024.
- 8 Ware, Jacob. « [Terrorist Groups, Artificial Intelligence, and Killer Drones](#) ». War on the Rocks, 24 septembre 2019.
- 9 « [Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes](#) ». Centre des Nations Unies pour la lutte contre le terrorisme et Institut interrégional de recherche des Nations unies sur la criminalité et la justice, 2021.
- 10 Kreps, Sarah. « [Democratizing Harm: Artificial Intelligence in The Hands of Nonstate Actors](#) ». Brookings, novembre 2021.

© Sa Majesté le Roi du chef du Canada, 2025

Pour obtenir des informations sur les droits de reproduction : <https://horizons.gc.ca/fr/contactez-nous/>

PDF : PH4-212/2025F-PDF

ISBN : 978-0-660-76884-7

Also available in English under the title: AI could empower non-state actors and overwhelm security organizations.

AVERTISSEMENT

Horizons de politiques Canada (Horizons de politiques) est le centre d'excellence en prospective du gouvernement du Canada. Notre mandat est de doter le gouvernement du Canada d'une perspective et d'un état d'esprit tournés vers l'avenir afin de renforcer la prise de décisions. Le contenu de ce document ne représente pas nécessairement le point de vue du gouvernement du Canada ou des agences et ministères participants.